

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

2022 APR 19 PM 3:09

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)SEVEN (7) ELECTRONIC DEVICES CURRENTLY  
STORED IN THE EVIDENCE VAULT AT ODPS, 9476  
MERIDIAN WAY, WEST CHESTER, OH 45069

Case No.

U.S. DISTRICT COURT  
SOUTHERN DISTRICT OHIO  
WESTERN DIV DAYTON

3.22 mj

1197

MAGISTRATE JUDGE GENTRY

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the \_\_\_\_\_ District of \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

SEE ATTACHMENT C

The application is based on these facts:

SEE ATTACHED AFFIDAVIT AND ATTACHMENT D

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA GREGORY E. ENGELHARD, USDA-OIG

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/19/2022

City and state: DAYTON, OHIO



Judge's signature

CAROLINE H. GENTRY, U.S. MAGISTRATE JUDGE

Printed name and title

**ATTACHMENT "A"**

**Property/Location to be Searched**

The following items of evidence were seized on April 12, 2022 from a residence located at 8471 Rodebaugh Road, Reynoldsburg, Ohio 43068 during the execution of a search warrant of said premises and are presently being stored and secured in the evidence vault of the Ohio Department of Public Safety's Offices, located at 9476 Meridian Way, West Chester, Butler County, Ohio 45069.

- # 1     Black Samsung Cell Phone (passcode 7979)
- # 2     Black Samsung Cell Phone in gold case
- # 3     Black Samsung Cell Phone in black case
- #18     White HP laptop S/N CND426CNBT
- # 20     Pink iPhone
- #24     Black iPhone with black case/charger
- #25     White Samsung phone in black/white case

**ATTACHMENT “B”**

**Specific Items to be Searched on Listed Electronic Device**

1. All stored data and information contained on the electronic device(s) described and listed in Attachment “A” that relate to criminal violations listed in paragraph 3 of the supporting affidavit that may have occurred between on or about June 1, 2011 and continuing until on or about April 12, 2022.

2. Evidence of user attribution showing who used or owned the electronic device(s) at the time the various data and information described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of any Internet Protocol address to communicate with persons such as co-conspirators, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records,” “data” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT C

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §§ 371 & 1349	Conspiracy to Defraud the United States and Commit Wire Fraud
7 U.S.C. § 2024(b) & (c)	Unauthorized Use, Transfer, Acquisition or Possession of SNAP Benefits
18 U.S.C. § 641	Theft of Public Money
18 U.S.C. § 1001	Making a False Statement
18 U.S.C. § 1029	Access Device Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft
42 U.S.C. § 1383(a)	Supplemental Security Income Fraud

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF  
SEIZED ELECTRONIC MEDIA LISTED IN  
ATTACHMENT “A”, AND CURRENTLY  
LOCATED AT THE OHIO DEPARTMENT  
OF PUBLIC SAFETY’S EVIDENCE  
VAULT, LOCATED AT 9476 MERIDIAN  
WAY, WEST CHESTER, BUTLER  
COUNTY, OHIO 45069

Case No. \_\_\_\_\_

3:22 mj 119

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER  
RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Gregory E. Engelhard, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of certain property—to wit: electronic devices—(listed in Attachment “A”). These electronic devices were previously seized by law enforcement agents on April 12, 2022, and are currently in law enforcement possession. This Application seeks permission to extract from said property electronically stored data and information described in Attachment “B”.

2. I am a Special Agent (SA) with the United States Department of Agriculture (USDA), Office of Inspector General (OIG) and have been so employed since March, 2005. I hold both a Bachelor’s and Master’s degree. I am also a graduate of the Federal Law Enforcement Training Center, in Glynco, GA. I have over 28-years of law enforcement experience as both a local police officer and a SA with the USDA-OIG. My duties as a SA with the USDA-OIG have included participating a variety of investigations concerning: Food Stamp Program fraud (currently referred to as the Supplemental Nutrition Assistance Program or

“SNAP”) fraud, Women, Infant and Children (WIC) Food and Nutrition Program fraud, complex federal program benefits fraud, money laundering schemes, embezzlement schemes, organized extortion rings, smuggling schemes and illicit animal fighting operations. I have also received extensive and specialized training in the areas of financial crimes, the illicit use of access devices, wire fraud schemes and money laundering violations.

3. I am currently a member of the Southern District of Ohio Financial Crimes Task Force (SDOHTF). This task force is made up of representatives from various law enforcement agencies to include the USDA-OIG, the United States Secret Service (USSS), the Social Security Administration, Office of the Inspector General (SSA-OIG) and the Ohio Department of Public Safety (ODPS) Investigative Unit. The SDOHTF is presently engaged in an investigation of MARQUIS DESADE FARMER of Columbus, Ohio which involves suspected violations of federal law to include: Conspiracy to Defraud the United States and Commit Wire Fraud, in violation of 18 U.S.C. §§ 371 and 1349; Unauthorized Use, Transfer, Acquisition, Alteration, or Possession of Food Stamp Benefits, in violation of 7 U.S.C. § 2024 (b) and (c); Theft of Public Money, in violation of 18 U.S.C. § 641; Access Device Fraud, in violation of 18 U.S.C. § 1029; Wire Fraud, in violation of 18 U.S.C. § 1343; Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A, Making False Statements, in violation of 18 U.S.C. § 1001; and Supplemental Security Income Fraud, in violation of 42 U.S.C. § 1383(a).

4. This affidavit is intended to establish the existence of sufficient probable cause for the requested warrant and does not set forth all of my knowledge involving this investigation.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

5. The electronic device(s) to be searched are listed in Attachment “A” of this application. Each of the subject electronic devices are currently located in the evidence vault

maintained at the Ohio Department of Public Safety's Offices, 9476 Meridian Way, West Chester, Butler County, Ohio 45069.

6. The applied-for warrant would authorize the forensic examination of the aforesaid listed electronic devices for the purpose of identifying any and all relevant electronically stored data and other information that may be stored on them.

### **PROBABLE CAUSE**

7. On March 31, 2022, your Affiant telephonically appeared before U.S. Magistrate Judge Peter B. Silvain Jr. of the Southern District of Ohio (hereinafter referred to as "SDOH") sitting in Dayton, Ohio for the purpose of filing applications for four (4) search warrants and an arrest warrant for MARQUIS DESADE FARMER. The four search locations were: the residence of MARQUIS DESADE FARMER, located at 3216 Marion Place, Columbus, Ohio 43227; the residence of BEYENE T. GOITAM and MAKDA BERHANE, located at 8471 Rodebaugh Road, Reynoldsburg, Ohio 43068; the commercial business establishment known as AGLER MARKET, located at 2043 Agler Road, Columbus, Ohio 43224; and a 2010 Mercedes-Benz S550 automobile, black in color, bearing Ohio registration 1PRITB, (VIN# WDDNG7BB6AA357807). As part of the warrant application process, your Affiant filed a joint supporting affidavit, a copy of which is attached herewith and marked as Attachment "D" to this affidavit. Magistrate Judge Silvain ultimately granted the requested search warrants.

8. Your Affiant specifically adopts, re-alleges and re-asserts all the facts contained in the March 31, 2022 SDOH supporting search affidavit which is marked as Attachment "D" and incorporated as part of this affidavit.

9. On April 12, 2022, law enforcement officials associated with the SDOHTF executed the aforesaid warrants at the various locations listed in the respective warrants in

Columbus, Ohio. As a result, SDOHTF officers seized various the electronic devices listed in Attachment “A”. While law enforcement authorities might already have all necessary legal authority to examine the said electronic devices, your Affiant seeks this additional warrant out of an abundance of caution to ensure that any subsequent forensic examination of the said devices will comply with all Fourth Amendment requirements and other federal laws.

10. The electronic devices remain securely stored to date at the Ohio Department of Public Safety’s Offices located at 9476 Meridian Way in West Chester, Butler County, Ohio 45069. Based upon your Affiant’s prior training and experience, I know that these devices have been stored in a manner such that their contents are, to the extent material to this investigation, in substantially the same state as when the devices first came into the possession of law enforcement authorities.

### **TECHNICAL TERMS**

11. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a

variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. **PDA:** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

12. Based on my prior training, experience, and research, I know that electronic devices have the capability of storing electronic data and information such as: customers names, addresses, business records, accounting records, electronic transactions, digital images of documents, etc.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

13. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

14. There is probable cause to believe that things that were once stored on an electronic device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

15. *Forensic evidence.* As further described in Attachment “B”, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that may establish how a device may have been used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the subject devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim’s electronic device over the Internet, the individual’s electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

16. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the electronic device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

17. *Manner of execution.* Because this warrant seeks only permission to examine the listed electronic device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**

18. I submit that this affidavit (together with the facts and circumstances set forth in Attachment "D") supports probable cause for a search warrant authorizing the examination of the subject seized electronic device which is stored at the location described in Attachment "A" to seek the items described in Attachment "B".

### **REQUEST FOR SEALING**

19. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents are necessary because the warrant is relevant to an ongoing criminal investigation and not all of the targets of this investigation have been fully identified. Based upon my training and experience, I have learned that, online criminals have been known to actively search for criminal affidavits and search warrants via the

internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its overall effectiveness.

Respectfully submitted,

  
\_\_\_\_\_  
GREGORY E. ENGELHARD  
Special Agent  
USDA-OIG

Subscribed and sworn to before me  
on this 19<sup>th</sup> day of April, 2022.

  
\_\_\_\_\_  
CAROLINE H. GENTRY  
UNITED STATES MAGISTRATE JUDGE